



Docket No.: 22040-00037-US1  
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:  
Makoto Izawa et al.

Application No.: 10/710,982

Confirmation No.: 4981

Filed: August 16, 2004

Art Unit: N/A

For: ENCRYPTION APPARATUS, ENCRYPTION  
METHOD, AND ENCRYPTION SYSTEM

Examiner: Not Yet Assigned

**CLAIM FOR PRIORITY AND SUBMISSION OF DOCUMENTS**

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Dear Sir:

Applicant hereby claims priority under 35 U.S.C. 119 based on the following prior foreign application filed in the following foreign country on the date indicated:

<u>Country</u>	<u>Application No.</u>	<u>Date</u>
Japan	2002-134680	May 9, 2002

In support of this claim, a certified copy of the said original foreign application is filed herewith.

Applicant believes no fee is due with this response. However, if a fee is due, please charge our Deposit Account No. 22-0185, under Order No. 22040-00037-US1 from which the undersigned is authorized to draw.

Dated: August 17, 2004  
23525\_1

Respectfully submitted,

By Larry J. Hume  
Larry J. Hume

Registration No.: 44,163  
CONNOLLY BOVE LODGE & HUTZ LLP  
1990 M Street, N.W., Suite 800  
Washington, DC 20036-3425  
(202) 331-7111  
(202) 293-6229 (Fax)  
Attorney for Applicant

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されて  
る事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed  
with this Office.

出 願 年 月 日      2 0 0 2 年   5 月   9 日  
Date of Application:

出 願 番 号      特 願 2 0 0 2 - 1 3 4 6 8 0  
Application Number:  
[J P 2 0 0 2 - 1 3 4 6 8 0]

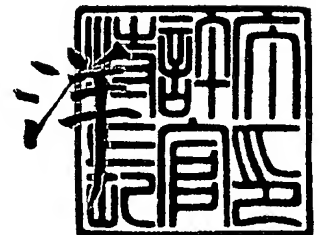
願      人  
Applicant(s):      新潟精密株式会社  
株式会社マイクロ総合研究所

CERTIFIED COPY OF  
PRIORITY DOCUMENT

2 0 0 4 年   7 月   5 日

特許庁長官  
Commissioner,  
Japan Patent Office

小 川



【書類名】 特許願

【整理番号】 14NS1428

【提出日】 平成14年 5月 9日

【あて先】 特許庁長官殿

【国際特許分類】 G09C 1/00

【発明者】

    【住所又は居所】 東京都品川区南品川 2 丁目 2 番 5 号 株式会社マイクロ  
                                総合研究所内

    【氏名】 井澤 誠

【発明者】

    【住所又は居所】 東京都品川区南品川 2 丁目 2 番 5 号 株式会社マイクロ  
                                総合研究所内

    【氏名】 成田 宏光

【発明者】

    【住所又は居所】 埼玉県上尾市緑丘 4 丁目 7 番 1 7 号

    【氏名】 岡本 明

【特許出願人】

    【識別番号】 591220850

    【氏名又は名称】 新潟精密株式会社

【特許出願人】

    【住所又は居所】 東京都品川区南品川 2 丁目 2 番 5 号

    【氏名又は名称】 株式会社マイクロ総合研究所

【代理人】

    【識別番号】 100105784

    【弁理士】

    【氏名又は名称】 橋 和之

    【電話番号】 049-249-5122

## 【手数料の表示】

【予納台帳番号】 070162

【納付金額】 21,000円

## 【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 0006161

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 暗号装置および方法、暗号システム

【特許請求の範囲】

【請求項 1】 複数のポートを有し、少なくとも 1つのポートに暗号処理機能を有する端末が直接または間接的に接続される暗号装置であって、

上記暗号処理機能を有する端末との間で暗号化によるセキュリティを終端するためにデータの暗号化処理および復号化処理を行う暗号／復号手段と、

上記複数のポートのうちのポートより入力され上記暗号／復号手段により暗号化処理または復号化処理が施されたデータを、ルーティング処理をすることなく他のポートにそのまま出力するブリッジ手段とを備えたことを特徴とする暗号装置。

【請求項 2】 上記暗号／復号手段は、上記暗号処理機能が導入された端末との間では暗号化されたデータの通信を行うとともに、上記暗号処理機能が導入されていない端末との間では暗号化されていないデータの通信を行うために上記暗号化処理および上記復号化処理を行うことを特徴とする請求項 1 に記載の暗号装置。

【請求項 3】 複数のポートを有し、少なくとも 1つのポートに暗号処理機能を有する端末が直接または間接的に接続される暗号装置であって、

上記複数のポートのうちのポートより入力され物理層およびデータリンク層を介して渡されたデータに対して暗号化処理または復号化処理を行う暗号／復号手段と、

上記暗号／復号手段により暗号化処理または復号化処理が施されたデータを、ネットワーク間のルーティング制御を行うネットワーク層に渡すことなくデータリンク層および物理層を介して他のポートより出力するようにするブリッジ手段とを備えたことを特徴とする暗号装置。

【請求項 4】 上記暗号化処理および上記復号化処理の制御に関する設定情報を記憶する設定情報記憶手段を備え、

上記暗号／復号手段は、上記設定情報記憶手段に記憶されている設定情報と、上記一のポートより入力されたパケットに付加されているヘッダ情報とを照合し

て上記暗号化処理および上記復号化処理の制御を行うことを特徴とする請求項 3 に記載の暗号装置。

【請求項 5】 複数のポートを有し、少なくとも 1 つのポートに暗号処理機能を有する端末が直接または間接的に接続される暗号装置において暗号化処理または復号化処理を行う方法であって、

上記複数のポートのうちのポートより入力され物理層およびデータリンク層を介して渡されたデータに対して暗号化処理または復号化処理を行い、これにより得られたデータを、ネットワーク間のルーティング制御を行うネットワーク層に渡すことなくデータリンク層および物理層を介して他のポートより出力するようにしたことを特徴とする暗号方法。

【請求項 6】 暗号処理機能が導入された端末と、請求項 1 に記載の暗号装置とが無線または有線のネットワークを介して接続されて成ることを特徴とする暗号システム。

【請求項 7】 暗号処理機能が導入された端末と、暗号処理機能が導入されていない端末との間に、請求項 2 に記載の暗号装置が無線または有線のネットワークを介して接続されて成ることを特徴とする暗号システム。

#### 【発明の詳細な説明】

##### 【0 0 0 1】

#### 【発明の属する技術分野】

本発明は暗号装置および方法、暗号システムに関し、特に、ネットワーク上で外部から攻撃されることによる情報の盗聴や改ざん等のリスクを低減するために情報の暗号化／復号化を行う装置および方法、これを適用したシステムに用いて好適なものである。

##### 【0 0 0 2】

#### 【従来の技術】

パーソナルコンピュータ（パソコン）をスタンドアロンで用いる場合は、パソコン内部の情報が盗み出されたり、改ざんされたり、破壊されたりする危険性は少ない。しかし、パソコンをインターネット等のネットワークに接続すると、やり取りされる情報は多くのネットワークをルーティングされていくことから、そ

の途中において盗聴や改ざん等の行われる危険性が一気に増大する。

#### 【0 0 0 3】

この問題を解決するための仕組みの1つとして、情報の暗号化がある。すなわち、送信側のパソコンで情報を暗号化して相手に送り、受信側のパソコンでこれを復号化して利用する。このようにすれば、ネットワークの途中で情報が盗聴されたとしても、情報が暗号化されているために、情報自体が見られる可能性が少なくなる。また、改ざんのリスクも低減される。

#### 【0 0 0 4】

##### 【発明が解決しようとする課題】

しかしながら、暗号を利用するためには、暗号通信しようとする端末の全てに専用の暗号ソフトをインストールし、様々な設定をしなければならない。ところが、各種端末が接続されるネットワークは、インターネットの他に、企業内のLAN（Local Area Network）なども存在する。そのLAN内には、プリンタやファクシミリなど物理的に暗号ソフトをインストールできない端末や、プリントサーバやデータベースサーバなど動作安定上等の問題から余分なソフトをインストールすることが好ましくない端末、OS（オペレーティングシステム）がなく単なるネットワークターミナルとして機能する端末なども存在する。そのため、一般的に企業内LANの中では、暗号を利用することは難しかった。

#### 【0 0 0 5】

ところが、LANの多くはインターネットに接続されており、必要に応じてLAN内のパソコンからインターネットにアクセスして情報のやり取りを行うことができるようになっている。しかし、このようにLANがインターネットに接続されていると、外部からの不正侵入や攻撃によって、LAN内部の機密情報が盗まれたり改ざんされたりする危険性が出てくる。

#### 【0 0 0 6】

そこで、アクセス権を持たない第三者がLAN内に不正に侵入するのを防ぐために、ファイアウォールが利用される。ファイアウォールは、一般的には1台のサーバをLANとインターネットとの接続部に用い、ここで専用のソフトウェアを動作させることによって機能する。しかし、ファイアウォールを設置しても、

ネットワーク上に存在するセキュリティホールを攻撃することによって不正侵入が行われることが少なくない。一旦不正侵入が行われると、内部の情報は暗号化されていないため、盗聴や改ざんが容易にできてしまうという問題があった。

#### 【0 0 0 7】

なお、従来、インターネット上に流れるデータをルーティングする中継機であるルータに暗号機能を持たせたものが存在する。例えばVPN (Virtual Private Network) ルータがそれである。このVPNルータを用いれば、端末に専用の暗号ソフトをインストールしなくても、VPNルータ間で暗号通信を行うことが可能となる。

#### 【0 0 0 8】

しかしながら、このVPNルータは、インターネットを利用して複数のLANを接続するために設けられる仮想専用線上の中継機として用いられるものである。そのため、LANどうしがやり取りする情報を途中のインターネット上において暗号化することはできるが、LAN内において情報を暗号化することはできないという問題があった。

#### 【0 0 0 9】

また、VPNルータにおいて暗号化を行うためには、ルータが必ず通信用のIPアドレスを持つことが必要となる。以下に、このことについて図8を用いて説明する。図8は、従来のVPNルータおよびこれに接続されるパソコンにおけるプロトコルの階層構造を示す図である。

#### 【0 0 1 0】

図8に示すように、通信しようとする2台のパソコン101, 102はそれぞれ1つのポート105, 106を有し、その中継機となるVPNルータ103, 104はそれぞれ2つのポート(107, 108), (109, 110)を有している。VPNルータ103の各ポート107, 108に対して物理層、MAC層(データリンク層)、IP-Secが個別に設けられ、各ポート107, 108に共通なものとしてIP層(ネットワーク層)、TCP/UDP層(トランスポート層)が設けられている。VPNルータ104の各ポート109, 110についても同様である。



**【 0 0 1 1 】**

層が深くなるほどユーザからは遠くなり、逆に層が浅くなるほどユーザに近くなる。各パソコン 1 0 1, 1 0 2 の I P 層よりも上位層には、T C P / U D P 層およびアプリケーション層（共に図示せず）が存在し、ユーザが使用するアプリケーションと下の層との橋渡しが行われる。

**【 0 0 1 2 】**

データの送信側では、上位層から下位層に向かって各層を通過するごとにデータが変換されるとともに、それぞれの層間でデータ伝送を可能にするためのヘッダが付加されていく。逆に、データの受信側では、各層宛てのヘッダを参照して各層で必要なデータが抽出される。そして、抽出されたデータは上位層へ引き渡され、最終的にアプリケーション層を介してユーザに届けられる。

**【 0 0 1 3 】**

以下に、それぞれの層の機能について説明する。T C P / U D P 層は、データを渡すべきアプリケーションの特定や、パケットの状態の管理などを行うレイヤである。データ送信側においては、上位層（アプリケーション層）から渡されたデータを相手のどのアプリケーションに渡すべきかを認識し、宛先ポート番号をデータに付加して下位層（ネットワーク層）に渡す。一方、データ受信側においては、下位層から渡されたパケットについて、通信の状態等によって抜けが生じていないかどうかを監視する。

**【 0 0 1 4 】**

I P 層は、複数のネットワークにまたがった端末間のデータ転送あるいはデータ中継に関する取り決めや制御を行うためのレイヤである。通信相手となる送信側と受信側のパソコン 1 0 1, 1 0 2 にはそれぞれ異なる I P アドレス①, ⑥が割り振られており、これらを明確にすることによって、end to endによる論理的な通信経路が決定する。2 つのポート（1 0 7, 1 0 8）, （1 0 9, 1 1 0）を有する V P N ルータ 1 0 3, 1 0 4 の場合、I P アドレスはポート毎に別個に割り振られる。

**【 0 0 1 5 】**

M A C（Media Access Control）層は、隣接機器のノード間で信頼性の高いデ

ータ伝送を保証するためのレイヤであり、製造段階で各機器に割り当てられた物理的なMACアドレスを有する。データ送信側においては、IP層で通信相手のIPアドレスが明確になると、その下位に位置するMAC層において、確立された相手のIPアドレスをもとに、経由する次の機器（物理的に接続されている隣接ノード）の宛先を決定する。一方、データ受信側においては、MACアドレスをもとに自分宛のパケットであることを認識した後、その上位層のIP層でIPアドレスを解析し、そのパケットを他の機器に対して更にルーティングするか自分に取り込むかを判断する。

#### 【0016】

物理層は、上位層から渡されたデータを電気信号や光信号に変換し、同軸ケーブルや光ファイバケーブル等の伝送媒体111を介して実際のデータ伝送を行ったり、伝送媒体111から送られてきた電気信号や光信号を上位層で認識可能なデータに変換し、それを上位層に渡したりするためのレイヤである。物理層の上位層であるMAC層では、物理層の通信インタフェースに依存した手法に従って上述の処理を行う。

#### 【0017】

IP-Secは、データの暗号化処理および復号化処理を行う機能部である。すなわち、MAC層からIP層に渡されるデータを取得して、当該データの暗号化処理および暗号の復号化処理を行う。

#### 【0018】

このような階層構造を有するVPNルータ103、104を用いてパソコン101、102間で暗号通信を行う場合、VPNルータ103では、例えば一方のパソコン101から他方のパソコン102宛てに送られてきたIPパケットを第1のポート107で受信し、IP層までパケットを順次引き渡して分解する。このとき、パケット中から抽出したデータをIP-Secで暗号化する。そして、パケットヘッダ中に含まれている宛先IPアドレスをもとに、ルータ自身が持つルーティングテーブルを参照して次の転送ノードを決定し、IP層から物理層へと再度パケットを組み立てて第2のポート108から送出する。

#### 【0019】

VPNルータ103の第2のポート108から出力された暗号化パケットは、VPNルータ104の第1のポート109で受信される。VPNルータ104は、受信した暗号化パケットをIP層まで順次引き渡して分解し、パケット中から抽出したデータをIPsecで復号化する。そして、パケットヘッダ中に含まれている宛先IPアドレスをもとに、ルータ自身が持つルーティングテーブルを参照して次の転送ノードを決定し、IP層から物理層へと再度パケットを組み立てて第2のポート110から送出する。

#### 【0020】

この第2のポート110から出力されたIPパケットは、パソコン102で受信される。この受信されたIPパケットは物理層、MAC層、IP層を介して上位層へと順次引き渡されて分解され、最終的に図示しないアプリケーション層を介してユーザにデータが届けられる。以上の手順により、パソコン101、102が暗号ソフトを備えていなくても、VPNルータ103、104間で暗号通信をすることが可能となる。

#### 【0021】

図8に示したシステムの場合、VPNルータ103、104の両側に異なるネットワーク（パソコン101を有するネットワークAとパソコン102を有するネットワークB）が存在し、これが集まってインターネットを構成している。そのため、それぞれのネットワーク毎に異なるネットワークアドレスが割り振られる。よって、これらの異なるネットワーク間をルーティング（経路選択、場合によってパケットの破棄、パケットの分割あるいは統合等）するVPNルータ103、104も、異なるIPアドレスを持つことが必須であり、そのために煩雑なアドレス設定作業を行わなければならないという問題があった。

#### 【0022】

また、VPNルータ103、104では第1のポート107、109に接続されるネットワークと第2のポート108、110に接続されるネットワークは一般的に異なるものであり、そのためにポート毎に異なるIPアドレスを設定する必要がある。よって、VPNルータ103、104の入力と出力とでIPアドレスが変わってしまう。そのため、ネットワーク上にある端末間にVPNルータを

挿入したり、あるいは端末間からVPNルータを外したりする際には、VPNルータ自身のアドレス設定を行うだけでなく、当該VPNルータに接続される端末のアドレス設定も変更する必要がある、各種の煩雑な作業を行わなければならないという問題があった。

#### 【0023】

例えば、図8の例においてVPNルータ103、104を接続しない状態で通信を行う場合は、パソコン101、102は同一のネットワーク内に存在することになるので、ネットワークアドレスが共に同じとなり、パソコン101、102間で直接の通信が可能である。この場合、パソコン101からパソコン102に送信するパケットのIPアドレスは、図9（a）のようになる。すなわち、送信側であるパソコン101の送信元IPアドレス①と、受信側であるパソコン102の宛先IPアドレス⑥のネットワークアドレスには、同じネットワークアドレスAを設定すれば良い。

#### 【0024】

これに対し、パソコン101とパソコン102との間にVPNルータ103、104を挿入した場合は、送信されるパケットのIPアドレスは図9（b）のようになる。すなわち、パソコン101、102は異なるネットワークに存在することになるので、送信元IPアドレス①と宛先IPアドレス⑥には、異なるネットワークアドレスA、Bを設定しなければならない。

#### 【0025】

このように、パソコン101とパソコン102との間にVPNルータ103、104を挿入したり、あるいはその逆にVPNルータ103、104を取り外したりすると、パソコン101、102の属するネットワークが変わる。したがって、それに合わせて、パソコン101、102のデフォルトゲートウェイのアドレス（自分と異なるネットワークに対して通信をする場合の宛先IPアドレス（VPNルータ103、104のポート107、110））や、パソコン101、102の何れかのIPアドレスの設定を変更する必要があるが生じる。

#### 【0026】

以上のように、従来のVPNルータでは、その接続の有無によって透過性を保

つことが困難であり、システムの導入時やメンテナンス時には多大な作業をしなければならないという問題があった。

#### 【 0 0 2 7 】

本発明は、このような問題を解決するために成されたものであり、専用の暗号ソフトをインストールできない端末を有する企業内 L A N の中でも暗号を利用して、外部からの不正侵入や攻撃によって L A N 内部の機密情報が盗まれたり改ざんされたりする危険性を低減できるようにすることを目的とする。

また、本発明は、アドレス設定などの煩雑な作業を行うことなく、企業内 L A N で暗号を利用できるようにすることを目的とする。

#### 【 0 0 2 8 】

##### 【課題を解決するための手段】

本発明の暗号装置は、複数のポートを有し、少なくとも 1 つのポートに暗号処理機能を有する端末が直接または間接的に接続される暗号装置であって、上記暗号処理機能を有する端末との間で暗号化によるセキュリティを終端するためにデータの暗号化処理および復号化処理を行う暗号／復号手段と、上記複数のポートのうちのポートより入力され上記暗号／復号手段により暗号化処理または復号化処理が施されたデータを、ルーティング処理をすることなく他のポートにそのまま出力するブリッジ手段とを備えたことを特徴とする。

#### 【 0 0 2 9 】

本発明の他の態様では、上記暗号／復号手段は、上記暗号処理機能が導入された端末との間では暗号化されたデータの通信を行うとともに、上記暗号処理機能が導入されていない端末との間では暗号化されていないデータの通信を行うために上記暗号化処理および上記復号化処理を行うことを特徴とする。

#### 【 0 0 3 0 】

本発明のその他の態様では、複数のポートを有し、少なくとも 1 つのポートに暗号処理機能を有する端末が直接または間接的に接続される暗号装置であって、上記複数のポートのうちのポートより入力され物理層およびデータリンク層を介して渡されたデータに対して暗号化処理または復号化処理を行う暗号／復号手段と、上記暗号／復号手段により暗号化処理または復号化処理が施されたデータ

を、ネットワーク間のルーティング制御を行うネットワーク層に渡すことなくデータリンク層および物理層を介して他のポートより出力するようにするブリッジ手段とを備えたことを特徴とする。

#### 【0031】

本発明の更に別の態様では、上記暗号化処理および上記復号化処理の制御に関する設定情報を記憶する設定情報記憶手段を備え、上記暗号／復号手段は、上記設定情報記憶手段に記憶されている設定情報と、上記一のポートより入力されたパケットに付加されているヘッダ情報とを照合して上記暗号化処理および上記復号化処理の制御を行うことを特徴とする。

#### 【0032】

また、本発明の暗号方法は、複数のポートを有し、少なくとも1つのポートに暗号処理機能を有する端末が直接または間接的に接続される暗号装置において暗号化処理または復号化処理を行う方法であって、上記複数のポートのうちのポートより入力され物理層およびデータリンク層を介して渡されたデータに対して暗号化処理または復号化処理を行い、これにより得られたデータを、ネットワーク間のルーティング制御を行うネットワーク層に渡すことなくデータリンク層および物理層を介して他のポートより出力するようにしたことを特徴とする。

#### 【0033】

また、本発明の暗号システムは、暗号処理機能が導入された端末と、請求項1に記載の暗号装置とが無線または有線のネットワークを介して接続されて成ることを特徴とする。

#### 【0034】

本発明の他の態様では、暗号処理機能が導入された端末と、暗号処理機能が導入されていない端末との間に、請求項2に記載の暗号装置が無線または有線のネットワークを介して接続されて成ることを特徴とする。

#### 【0035】

##### 【発明の実施の形態】

以下、本発明の一実施形態を図面に基づいて説明する。

図1は、本実施形態の暗号装置を適用した暗号システムの全体構成例を示す図

である。

#### 【0 0 3 6】

図 1 において、1 は本実施形態の暗号装置であり、2 つのポートを有し、一方のポートにはネットワークプリンタ 2、DBサーバ 3、ネットワークターミナル 4 などのデバイスが接続され、他方のポートにはハブ 5 が接続されている。この暗号装置 1 は、ネットワークプリンタ 2、DBサーバ 3、ネットワークターミナル 4 などのデバイスと、ハブ 5 との間でデータの中継を行う。

#### 【0 0 3 7】

ネットワークプリンタ 2 は、暗号ソフトを物理的にインストールできない端末である。DBサーバ 3 は、動作安定上等の問題から余分な暗号ソフトをインストールすることが好ましくない端末である。ネットワークターミナル 4 は、OS がなく暗号ソフトを動作させることができない端末である。したがって、これらの端末 2 ～ 4 には暗号ソフトはインストールされていないものとする。

#### 【0 0 3 8】

また、ハブ 5 は、物理層においてデータの中継する機器であり、上述した暗号装置 1 の他に、無線通信用のアクセスポイント 6 とデスクトップパソコン 7 とが接続されている。すなわち、この場合のハブ 5 は、暗号装置 1 と、アクセスポイント 6 およびデスクトップパソコン 7 との間でデータの中継を行う。

#### 【0 0 3 9】

さらに、上記アクセスポイント 6 には、デスクトップパソコン 8 とラップトップパソコン 9 とが無線により接続されている。デスクトップパソコン 7、8 およびラップトップパソコン 9 には、データの暗号化および復号化を行うための暗号ソフトがインストール可能であり、実際にインストールされているものとする。

#### 【0 0 4 0】

このような構成により、暗号ソフトがインストールされていないネットワークプリンタ 2、DBサーバ 3 およびネットワークターミナル 4 と、暗号ソフトがインストールされているパソコン 7 ～ 9 との間で、暗号装置 1、ハブ 5 およびアクセスポイント 6 を介してデータ通信が行われる。

#### 【0 0 4 1】

その際、暗号装置 1 は、暗号ソフトがインストールされているパソコン 7 ～ 9 との間では暗号化されたデータの通信を行うとともに、暗号ソフトがインストールされていない端末 2 ～ 4 との間では暗号化されていないデータの通信を行うために暗号化処理および暗号の復号化処理を行う。

#### 【 0 0 4 2 】

例えば、デスクトップパソコン 7 からネットワークプリンタ 2 にデータを送出してプリントアウトするときは、まずデスクトップパソコン 7 にインストールされている暗号ソフトを用いてデータを暗号化し、ハブ 5 を介して暗号装置 1 に供給する。次に暗号装置 1 は、受け取ったデータを復号化し、ネットワークプリンタ 2 に送出する。

#### 【 0 0 4 3 】

また、例えば DB サーバ 3 にて管理されているデータをラップトップパソコン 9 に取り込むときは、DB サーバ 3 は、与えられる要求に応じて該当するデータを暗号装置 1 に供給する。この暗号化されていないデータを受け取った暗号装置 1 は、そのデータを暗号化し、ハブ 5 およびアクセスポイント 6 を介してラップトップパソコン 9 に送信する。ラップトップパソコン 9 は、受け取ったデータを復号化し、所望の処理に利用する。

#### 【 0 0 4 4 】

以上の説明から明らかなように、本実施形態の暗号装置 1 を用いることによって、専用の暗号ソフトをインストールできない端末 2 ～ 4 を有する企業内 LAN の中でも、暗号を利用することが可能となる。これにより、外部からの不正侵入や攻撃によって LAN 内部の機密情報が盗まれたり改ざんされたりする危険性が少ないセキュアなネットワーク 1 0 を構築することができる。

#### 【 0 0 4 5 】

なお、暗号装置 1 と各端末 2 ～ 4 との間において暗号は利用できないが、これらを繋ぐケーブル 1 1 は物理的に短い配線であり、この部分が外部アタックされることによって盗聴や改ざんが行われる可能性は極めて低いので、セキュリティ上で特に問題となることはない。

#### 【 0 0 4 6 】



図2は、本実施形態の暗号装置を適用した暗号システムの他の構成例を示す図である。なお、この図2において、図1に示した構成要素と同一の機能を有する構成要素には同一の符号を付している。図2に示すように、本実施形態の暗号装置1は、一方のポートにインターネット20が接続され、他方のポートにハブ5が接続されている。インターネット20の先には、図1に示したネットワークプリンタ2、DBサーバ3、ネットワークターミナル4などのように暗号ソフトをインストールできない端末、あるいは、パソコン7～9のように暗号ソフトがインストールされた端末が複数台接続されている。

#### 【0047】

図1に示した例では、1台の暗号装置1に対して1台のデバイスが接続されており、1台のデバイスに関する暗号／復号処理を1台の暗号装置1が専用で行っていた。すなわち、図1に示す暗号装置1は、暗号ソフトがインストールされたパソコン7～9と、暗号ソフトがインストールされていない1台のデバイスとの間に接続され、暗号ソフトがインストールされたパソコン7～9との間で暗号化によるセキュリティを終端していた。

#### 【0048】

これに対して、図2に示す例では、暗号装置1は、暗号ソフトがインストールされたパソコン7～9と、インターネット20に接続された複数台のデバイスとの間に接続されている。このように、本実施形態の暗号装置1は、複数台のデバイスに対して暗号化によるセキュリティを終端することも可能である。この場合、暗号装置1は、接続されているデバイスの数だけデータパスを有し、それぞれのデバイス毎に異なる暗号鍵で暗号／復号処理を行う。

#### 【0049】

上記複数台のデバイスは、暗号ソフトがインストールされていても良いし、インストールされていなくても良い。暗号ソフトがインストールされている場合には、セキュアネットワーク10の外部にあるインターネット20上でも暗号を利用することができる。なお、上記複数台のデバイスは、インターネット20を介して接続されている必要は必ずしもなく、暗号装置1に直接接続しても良い。この場合、暗号装置1は2つ以上のポートを有することになる。

## 【0 0 5 0】

図 3 は、本実施形態の暗号装置を適用した暗号システムの更に別の構成例を示す図である。なお、この図 3 において、図 1 に示した構成要素と同一の機能を有する構成要素には同一の符号を付している。図 3 に示す例も図 2 の例と同様に、1 台の暗号装置 1 が複数台のデバイスに対して暗号化によるセキュリティを終端する例である。

## 【0 0 5 1】

図 3 に示す例では、セキュアネットワーク 1 0 の内部は、3 台のパソコン 7 ～ 9 が全てアクセスポイント 6 に無線 LAN にて接続されている。アクセスポイント 6 は、暗号装置 1 を介してインターネット 2 0 に接続されている。

## 【0 0 5 2】

図 4 は、図 1 に示した暗号システムにおいて、暗号装置 1 およびこれに直接および間接的に接続される DB サーバ 3 およびラップトップパソコン 9 におけるプロトコルの階層構造を示す図である。図 4 に示す例では、DB サーバ 3 には暗号ソフトがインストールされておらず（IP-Se c がない）、ラップトップパソコン 9 には暗号ソフトがインストールされている（IP-Se c を有する）。この DB サーバ 3 およびラップトップパソコン 9 の間に、本実施形態の暗号装置 1 が接続されている。ここでは、DB サーバ 3 にて保存されているデータを暗号装置 1 に送り、ここでデータを暗号化してパソコン 9 に送るような利用形態を想定している。

## 【0 0 5 3】

図 4 に示すように、DB サーバ 3 およびパソコン 9 はそれぞれ 1 つのポート 3 1, 3 2 を有し、その中継機となる暗号装置 1 は 2 つのポート 3 3, 3 4 を有している。暗号装置 1 の各ポート 3 3, 3 4 に対して物理層および MAC 層（データリンク層）が個別に設けられ、各ポート 3 3, 3 4 に共通なものとして IP-Se c（暗号／復号処理機能）、IP 層（ネットワーク層）および TCP／UDP 層（トランスポート層）が設けられている。このように、本実施形態の暗号装置 1 は、IP-Se c により 2 つのポート 3 3, 3 4 間をブリッジさせているところに特徴がある。

**【0054】**

本実施形態の暗号装置 1 では、DBサーバ 3 とパソコン 9 との間におけるデータ転送に関しては IP 層および TCP/UDP 層は用いず、IP 層よりも下位層で処理を行う。すなわち、第 1 のポート 33 より入力されたデータに対して IP-Sec で暗号化処理を行い、それにより得られたデータを、IP 層にてルーティングすることなく（IP 層に渡すことなく）他方のポートにそのまま渡して出力する。

**【0055】**

すなわち、DBサーバ 3 にて作成されたパケットデータは、当該 DBサーバ 3 の MAC 層、物理層を通過して送信され、暗号装置 1 の第 1 のポート 33 より受信される。受信されたパケットデータは物理層、MAC 層を通過して IP-Sec に渡され、ここで暗号化処理が行われる。この暗号化されたパケットデータは、MAC 層および物理層を通過して第 2 のポート 34 より送信される。

**【0056】**

第 2 のポート 34 より送信されたパケットデータは、パソコン 9 で受信され、物理層、MAC 層を通過して IP-Sec に渡されて、暗号が復号化される。そして、復号化されたデータが IP 層を通過して図示しないアプリケーション層に渡される。これにより、DBサーバ 3 が暗号ソフトを備えていなくても、パソコン 9 に対して暗号化されたデータを送信することが可能となる。

**【0057】**

なお、本実施形態において IP 層および TCP/UDP 層は、暗号装置 1 自身に暗号化/復号化に関する各種の情報を設定する際に利用される。例えば、ある端末とある端末との間では暗号通信を行うが、他の端末との間では暗号通信を行わないなどといった暗号/復号処理の有無、ある端末とある端末との間ではパケットを破棄するなどといった通信の可否、暗号通信を行う場合における暗号化のレベル、暗号化を行う時間帯、暗号鍵などに関する種々の情報を暗号装置 1 に設定する場合には、IP 層および TCP/UDP 層を使用する。

**【0058】**

この種の設定情報は、IP-Sec ブリッジの機能によってメモリ上に保持さ

れる。IP-Secは、当該メモリに保持されている設定情報と、ポート33, 34より入力されたパケットに付加されているヘッダ情報（例えば、送信元IPアドレスおよび宛先IPアドレス）とを照合して、暗号／復号処理の制御などを行う。

#### 【0059】

このように、本実施形態の暗号装置1では、一のポートから入力されたデータをIP-Secで暗号化／復号化し、これにより得られたデータをIP層に渡すことなく、ルーティング処理をせずにそのまま他のポートに転送するようにしているので、データ通信時に暗号装置1のIPアドレスを不要とすることができる。すなわち、IPアドレスを持たずにIP層の暗号／復号処理を行うことが可能である。そのため、暗号装置1自身に対する煩雑なIPアドレス設定の必要をなくすることができる。

#### 【0060】

また、暗号装置1の両側に接続される端末は同じネットワークに属することになり、暗号装置1の入力ポートと出力ポートとでIPアドレスが変わることがなくなる。これにより、暗号装置1のネットワーク上における接続の有無に関わりなく、IPアドレスの透過性を保つことができる。すなわち、ネットワーク上に暗号装置1を接続したり、ネットワーク上から暗号装置1を外したりする際に、当該暗号装置1に接続される端末のアドレス設定も変更する必要がない。

#### 【0061】

例えば、図4のようにDBサーバ3とパソコン9との間に暗号装置1を挿入した場合も、暗号装置1を挿入せずにDBサーバ3とパソコン9との間で直接通信を行う場合も、DBサーバ3とパソコン9との間を流れるパケットのIPアドレスは、図5に示す通りのままで不変である。したがって、暗号装置1の接続の有無によってアドレス設定を何ら変更する必要がない。

#### 【0062】

これにより、ネットワークシステムの導入時やメンテナンス時には、本実施形態の暗号装置1を適当な箇所にただ挿入したり、あるいはただ取り外したりするだけ良くなり、煩雑なアドレス設定は行う必要がないので、作業負荷を大幅に削

減することができる。

#### 【0063】

さらに、本実施形態の場合、MACアドレスについても透過性を保つことができる。図6は、DBサーバ3からパソコン9にデータを送り、その間の暗号装置1でデータを暗号化する場合におけるパケットを示す図である。また、図7は、本実施形態との比較のために、図8に示す従来のシステムにおいて一方のパソコン101から他方のパソコン102にデータを送り、その間のVPNルータ103でデータを暗号化する場合におけるパケットを示す図である。

#### 【0064】

図6(a)および図7(a)は第1のポート33, 107にて受信するパケットを示し、図6(b)および図7(b)は第2のポート34, 108より送信するパケットを示す。なお、IPsecには、データ部のみを暗号化するトランスポートモードと、パケット全てを暗号化して更に新しいヘッダを追加するトンネルモードとがある。送信パケットに関しては、これら2つのモードについてそれぞれ示している。

#### 【0065】

図6から明らかなように、本実施形態によれば、IPアドレスだけでなく、MACアドレスについても第1のポート33と第2のポート34とで異なることなく、MACアドレスの透過性を保つことができる。すなわち、本実施形態の暗号装置1は、IPsecを有してデータの暗号／復号処理を行うことを除けば、一方のポートから入力されたデータを他方のポートにただ流すだけなので、データ通信時にはMACアドレスも不要とすることができる。

#### 【0066】

なお、以上に説明した実施形態は、本発明を実施するにあたっての具体化の一例を示したものに過ぎず、これによって本発明の技術的範囲が限定的に解釈されてはならないものである。すなわち、本発明はその精神、またはその主要な特徴から逸脱することなく、様々な形で実施することができる。

#### 【0067】

#### 【発明の効果】

本発明は上述したように、暗号処理機能が導入された端末との間で暗号化によるセキュリティを終端するために暗号化処理および暗号の復号化処理を行う暗号／復号手段を備えて暗号装置を構成し、この暗号装置をネットワークを介して端末に接続するようにしたので、専用の暗号ソフトをインストールできない端末を有する企業内LANの中でも暗号を利用することができるようになり、外部からの不正侵入や攻撃によってLAN内部の機密情報が盗まれたり改ざんされたりする危険性を低減することができる。

#### 【0068】

また、本発明では、暗号化処理または復号化処理が施されたデータを、ネットワーク間のルーティング制御を行うネットワーク層に渡すことなく出力するようにしたので、データ通信時に暗号装置のIPアドレスを不要とすることができる。また、暗号装置の入力ポートと出力ポートとでIPアドレスが変わることがなくなるので、暗号装置のネットワーク上における接続の有無に関わりなく、IPアドレスの透過性を保つことができ、暗号装置に接続される端末のアドレス設定に関しても変更の必要をなくすことができる。これにより、アドレス設定などの煩雑な作業を行うことなく、企業内LANで暗号を利用することができるようになる。

#### 【図面の簡単な説明】

##### 【図1】

本実施形態の暗号装置を適用した暗号システムの構成例を示す図である。

##### 【図2】

本実施形態の暗号装置を適用した暗号システムの他の構成例を示す図である。

##### 【図3】

本実施形態の暗号装置を適用した暗号システムの更に別の構成例を示す図である。

##### 【図4】

本実施形態による暗号装置およびこれに接続されるDBサーバおよびパソコンにおけるプロトコルの階層構造を示す図である。

##### 【図5】

本実施形態においてネットワーク上を流れるパケットの I P アドレスについて説明するための図である。

【図 6】

本実施形態の暗号装置を流れるパケットの M A C アドレスについて説明するための図である。

【図 7】

従来の V P N ルータを流れるパケットの M A C アドレスについて説明するための図である。

【図 8】

従来の V P N ルータおよびこれに接続されるパソコンにおけるプロトコルの階層構造を示す図である。

【図 9】

従来システムにおいてネットワーク上を流れるパケットの I P アドレスについて説明するための図である。

【符号の説明】

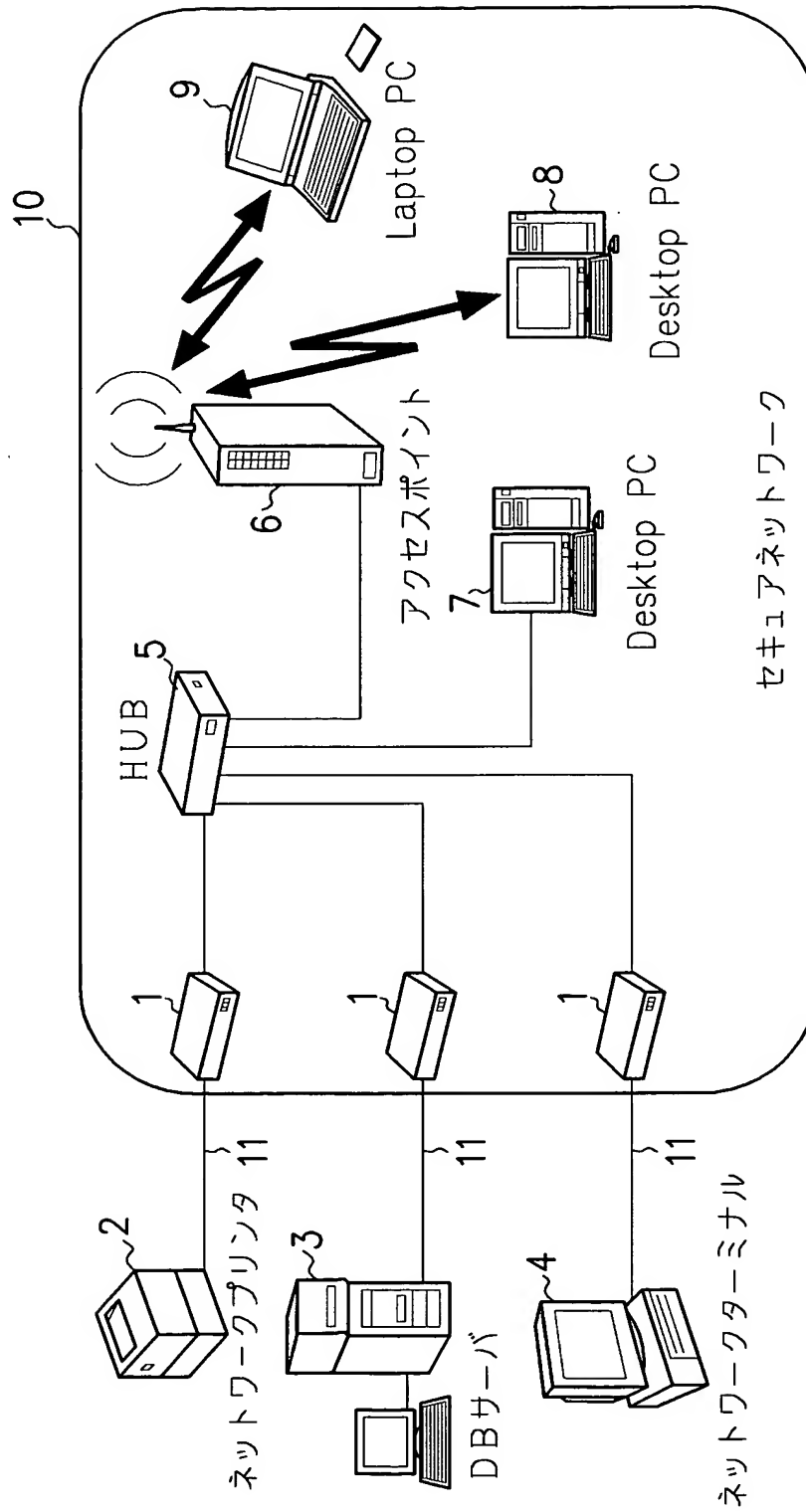
- 1 暗号装置
- 2 ネットワークプリンタ
- 3 D B サーバ
- 4 ネットワークターミナル
- 5 ハブ
- 6 アクセスポイント
- 7, 8 デスクトップパソコン
- 9 ラップトップパソコン
- 10 セキュアネットワーク
- 11 ケーブル
- 20 インターネット

【書類名】

図面

【図 1】

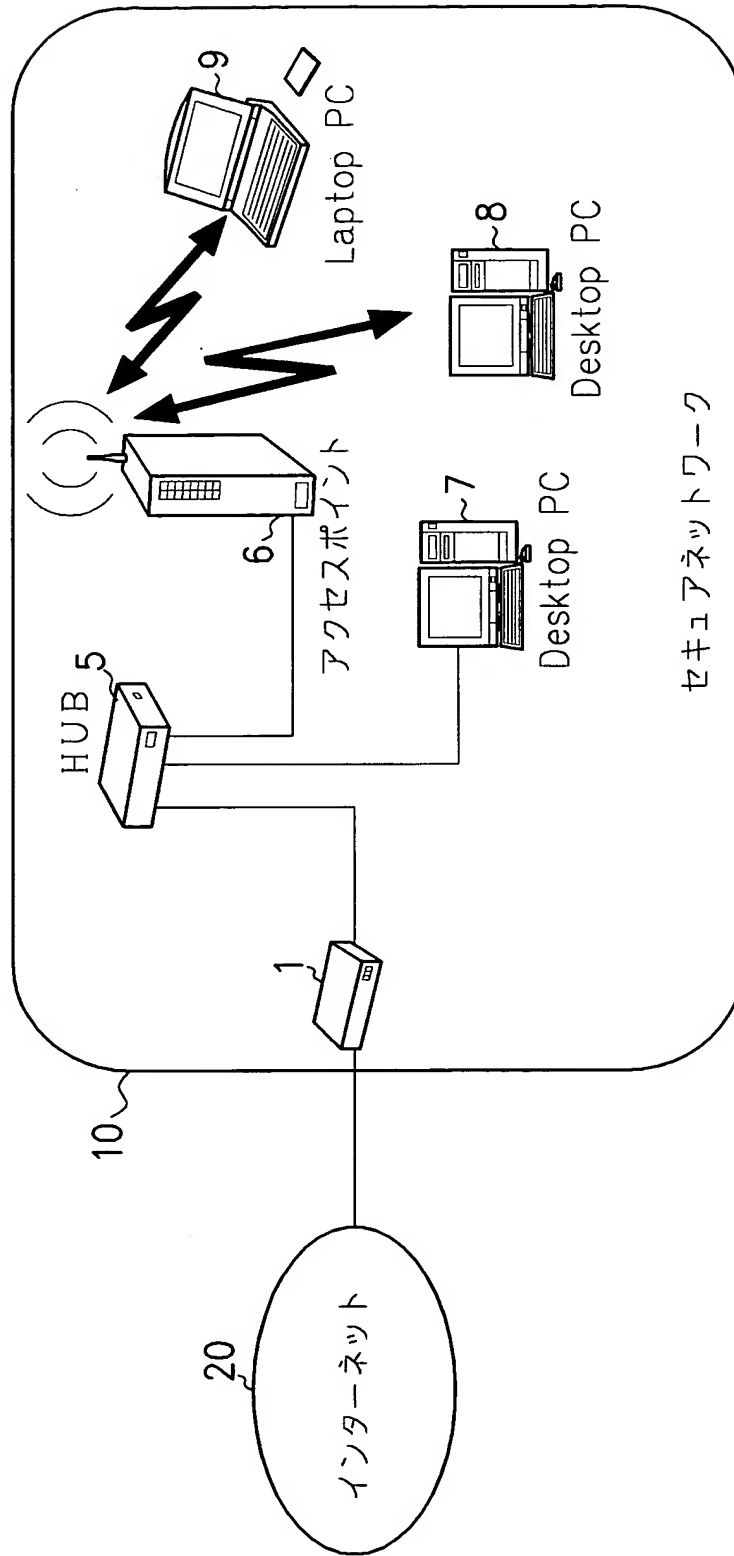
本実施形態による暗号システムの構成例



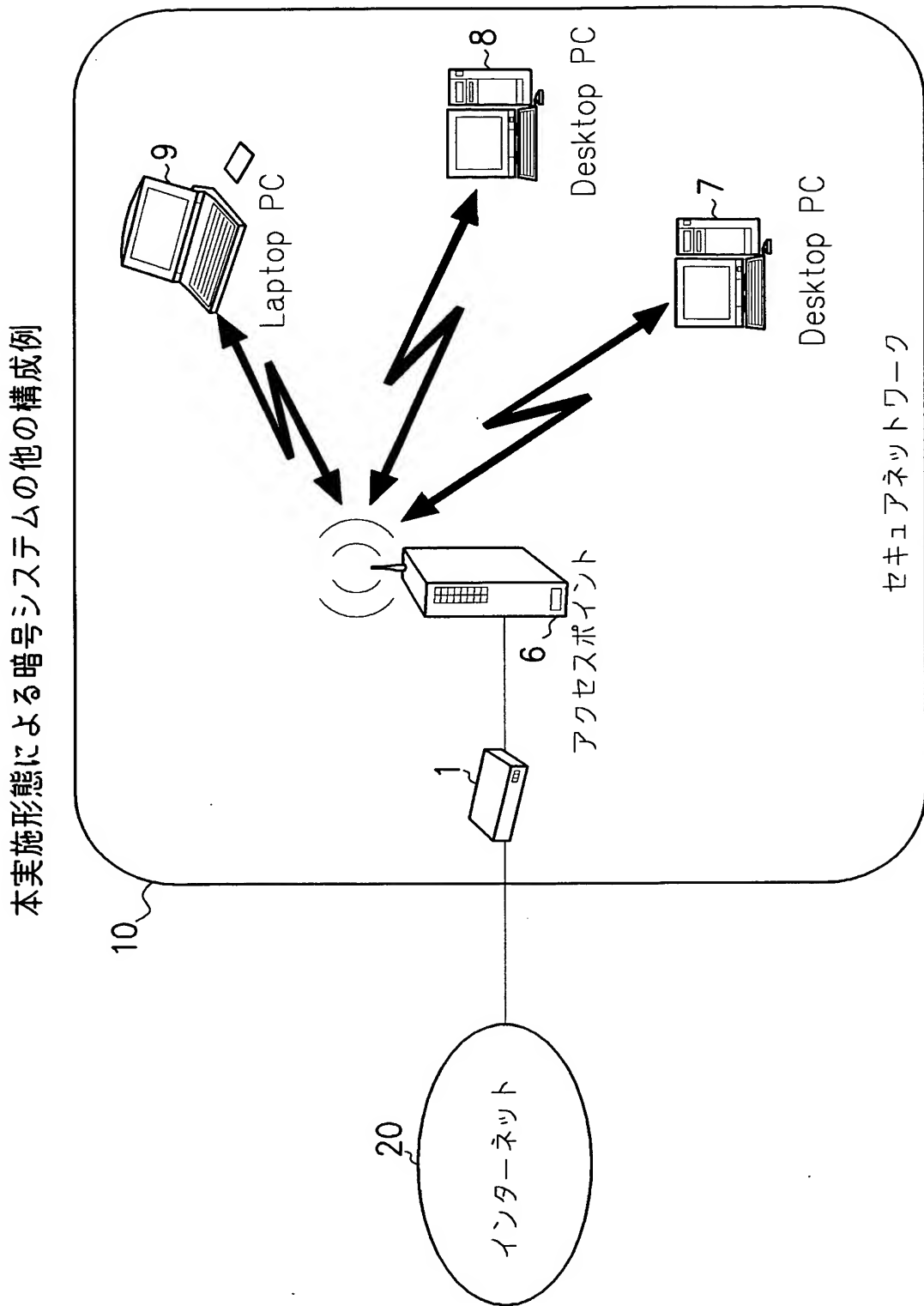


【図 2】

本実施形態による暗号システムの他の構成例

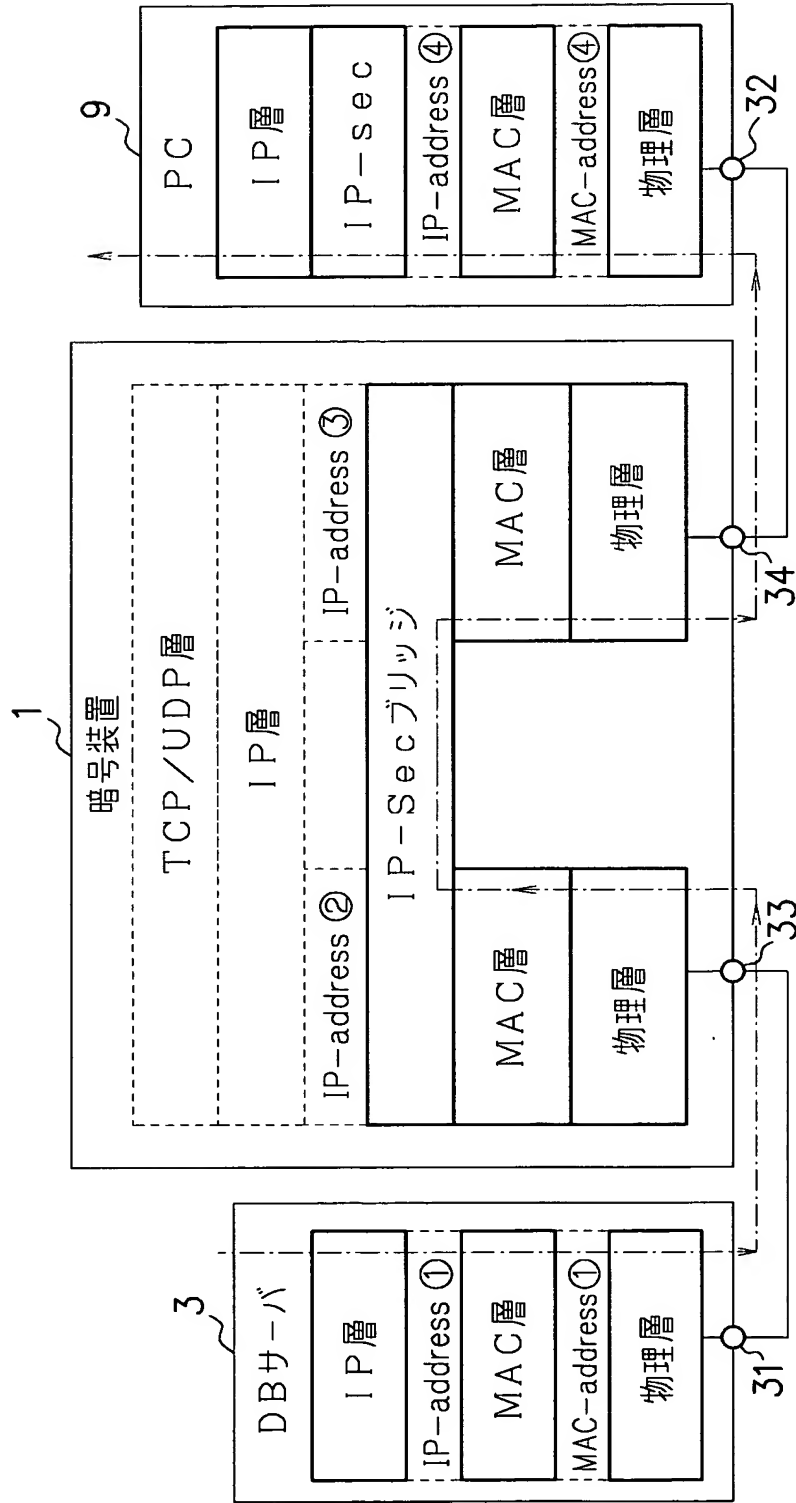


【図 3】



【図 4】

本実施形態による暗号装置のレイヤ構造



【図 5】

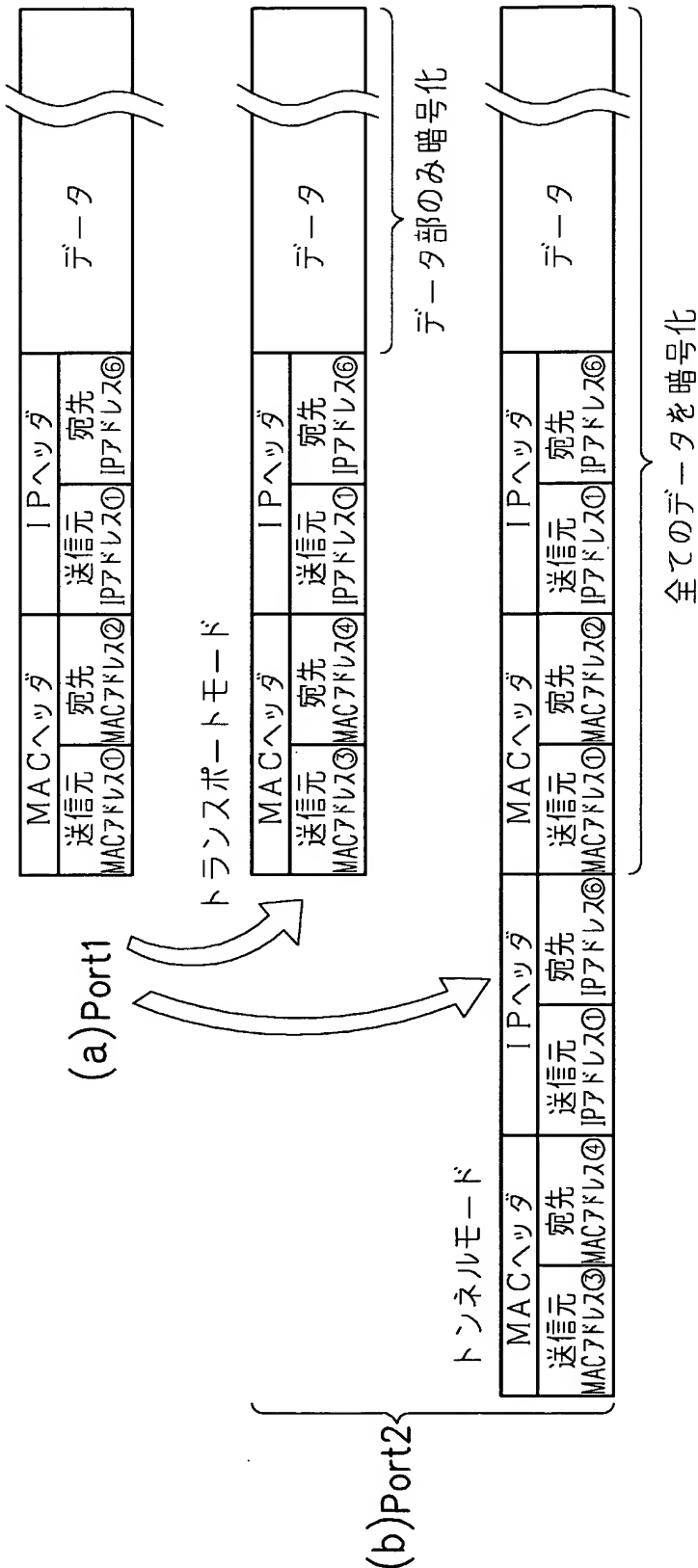
本実施形態のパケット

送信元 IP アドレス①		宛先 IP アドレス④		データ
ネットワークアドレス	ホストアドレス	ネットワークアドレス	ホストアドレス	
ネットワーク A	XXXXXXXX	ネットワーク A	XXXXXXXXXX	



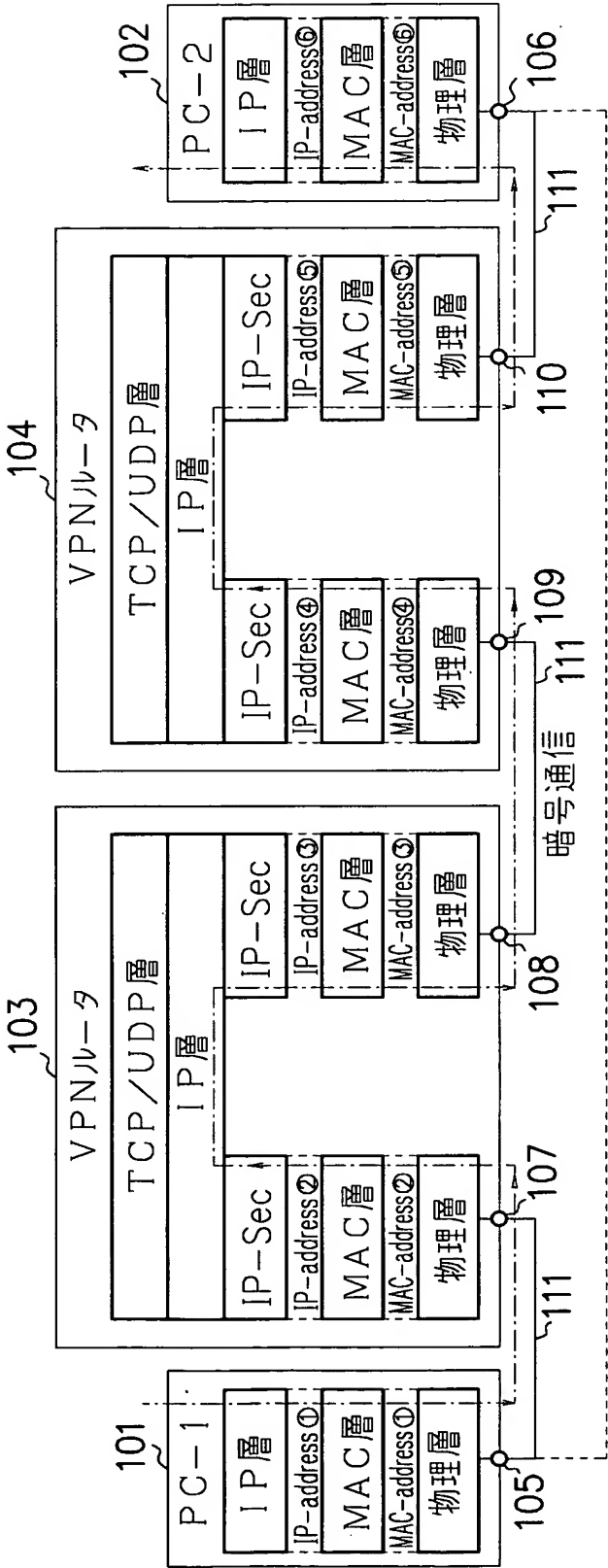
【図 7】

従来のVPNルータによるパケット



【図 8】

従来の VPN ルータのレイヤ構造



VPN ルータを入れない場合

【図 9】

VPNルータの有無によるパケットの違い

(a)	送信元 IP アドレス①		宛先 IP アドレス⑥		データ
	ネットワーク A	ホストアドレス	ネットワーク A	ホストアドレス	
	XXXXXXXX	XXXXXXXX	ネットワーク A	XXXXXXXXXX	
(b)	送信元 IP アドレス①		宛先 IP アドレス⑥		データ
	ネットワーク A	ホストアドレス	ネットワーク A	ホストアドレス	
	XXXXXXXX	XXXXXXXX	ネットワーク B	XXXXXXXXXX	



【書類名】 要約書

【要約】

【課題】 専用の暗号ソフトをインストールできない端末を有する企業内 L A N の中でも暗号を利用できるようにする。

【解決手段】 暗号ソフトがインストールされたパソコン 7 ～ 9 との間で暗号化によるセキュリティを終端するために暗号化处理および暗号の復号化处理を行う暗号装置 1 を設け、例えば暗号ソフトがインストールされていない端末 2 ～ 4 とパソコン 7 ～ 9 との間に接続することにより、専用の暗号ソフトをインストールできない端末 2 ～ 4 を有する企業内 L A N の中でも暗号を利用することができるようにして、外部からの不正侵入や攻撃によって L A N 内部の機密情報が盗まれる危険性が少ないセキュアなネットワーク 1 0 を構築することができるようにする。

【選択図】 図 1

特願 2 0 0 2 - 1 3 4 6 8 0

出 願 人 履 歴 情 報

識別番号

[ 5 9 1 2 2 0 8 5 0 ]

1. 変更年月日

1 9 9 6 年 5 月 9 日

[変更理由]

住所変更

住 所

新潟県上越市西城町 2 丁目 5 番 1 3 号

氏 名

新潟精密株式会社

特願 2 0 0 2 - 1 3 4 6 8 0

出 願 人 履 歴 情 報

識別番号

[ 5 0 1 3 0 6 9 7 7 ]

1. 変更年月日

2 0 0 1 年 8 月 2 日

[変更理由]

新規登録

住 所

東京都品川区南品川 2 丁目 2 番 5 号

氏 名

株式会社マイクロ総合研究所